Pinewood Security Operations Center (SOC)

24/7 in control

Door de hoge mate van digitalisering worden organisaties steeds meer afhankelijk van de IT-omgeving voor het uitvoeren van de dagelijkse operatie. Het lekken van gevoelige data door verschillende cyberdreigingen is een dagelijks risico met als gevolg dat de wet- en regelgeving steeds meer inzicht eist in de gebeurtenissen en maatregelen van datastromen binnen organisaties.

Het ontbreken van (voldoende) inzicht binnen de eigen (complexer wordende) netwerkinfrastructuur zorgt ervoor dat veel organisaties kwetsbaar worden voor (al dan niet) bewuste cyberaanvallen op de bedrijfskritische informatie en systemen met alle risico's van dien. Bijvoorbeeld het stilvallen van de operationele processen of het lekken van data wat mogelijk leidt tot financiële schade, boetes en imagoschade.

Pinewood zorgt ervoor dat organisaties controle krijgen over (kritische) informatiestromen en dat de informatiebeveiliging continue wordt aangepast naar de laatste ontwikkelingen wereldwijd. De afstemming tussen beleid en techniek is hierbij essentieel. Als 100% Nederlands bedrijf en specialist in informatiebeveiliging slaan de specialisten van Pinewood de brug tussen Techniek en Beleid, zodat complexe analyses uit techniek direct omgezet kunnen worden naar strategische en beleidsmatige maatregelen. Vanuit het Security Operations Center (SOC) hanteert Pinewood deze 2 aspecten als uitgangspunt. Dit betekent dat Pinewood niet alleen detecteert en analyseert, maar ook een adviserende rol heeft. Als uw security partner zorgt Pinewood ervoor dat u meer inzicht en grip krijgt op uw informatiebeveiliging.

Hoe werkt het Security Operations Center?

Een team van hoog opgeleide securityanalisten (hbo/wo) houdt uw systemen en netwerk 24x7x365 in de gaten. Op basis van de informatie verzameld door sensoren vindt in het SOC een analyse plaats van alle aan security gerelateerde gebeurtenissen in uw netwerk. Daarbij wordt door de analisten o.a. gebruik gemaakt van de meest actuele Threat Intelligence informatie uit zowel publieke als besloten bronnen wereldwijd. Naast verschillende automatische analyses worden incidenten ook in diepte onderzocht door middel van ''Security Intelligence''. De security specialisten van Pinewood hebben de expertise in huis om actief op zoek te gaan naar cyberdreigingen zoals infecties of geavanceerde hackpogingen door middel van "Threat Hunting".

Daarnaast heeft u vanuit gepersonaliseerde live dashboards (aangepast op de normen die voor uw sector van toepassing zijn, bijvoorbeeld ISO27001 of NEN7510) direct inzicht in het huidige beveiligingsniveau van uw infrastructuur.

In samenwerking met een security officer en analist wordt op basis van de geïdentificeerde security incidenten gezocht naar maatregelen om het beveiligingsniveau van uw organisatie doorlopend te

verhogen, zowel technisch als beleidsmatig. In periodiek terugkerende overleggen worden opgeleverde rapportages met u besproken en eventueel bijgestuurd naar uw doelstellingen.

Hoe worden de security incidenten gedetecteerd?

Voor het inrichten van de Security Monitoring dienst worden sensoren geplaatst in de infrastructuur van uw organisatie welke merk/platformonafhankelijk metingen kunnen verrichten en niet direct gebonden zijn aan een vooraf gesteld aantal gebruikers. Daarnaast kunnen sensoren met elkaar communiceren, waardoor bij het toevoegen van nieuwe locaties eenvoudig kan worden opgeschaald. Hierdoor ontstaat flexibiliteit, continuïteit, stabiliteit en is het mogelijk securitycomponenten te vervangen of toe te voegen zonder dat dit direct grote invloed heeft op de operatie.

Pinewood maakt altijd voor haar SOC diensten gebruik van twee type sensoren, zodat securityvraagstukken tot in de diepte (gecorreleerd) onderzocht kunnen worden en dat zelfs bij het toenemende gebruik van encryptie inzicht in data behouden blijft.

Logsensor
De logsensor verzamelt log- en eventinformatie van (beveiligings)componenten in de infrastructuur. Deze sensor kan tevens inzicht geven in de end to end events op het moment dat encryptie wordt toegepast.

Netwerksensor De netwerksensor verzamelt netwerkverkeer en geeft informatie over verdachte verkeersstromen zoals Ransomware en zero-day bedreigingen.

Standaard inbegrepen in het SOC:

- Plaatsing van sensoren en aanleg koppeling naar het Security Operations.
- 24x7x365 detectie van security incidenten in log- en en-event informatie.
- 24x7x365 Incident respons en mitigatieadvies van kritieke incidenten.
- 24x7 Toegang tot security dashboard voor inzage in dreigingsniveau en detailinformatie.
- Maandelijkse en kwartaal maatwerkrapportages op technisch en beleidsmatig niveau.
- Security Bulletins met informatie en advies over actuele dreigingen.
- Indien van toepassing on site consultant met informatie en advies over actuele dreigingen.
- Regelmatig overleg op operationeel, tactisch en strategisch niveau.
- Concrete maatregelen zowel technisch als organisatorisch
- 100% Nederlandse entiteit en standaard communicatie in het Nederlands

Flexibiliteit en maatwerk is het uitgangspunt van het Pinewood SOC. Samen met u richt Pinewood “uw SOC” in naar uw wensen en behoefte, zodat de dienstverlening past binnen uw (organisatie)doelstellingen.

CONTACT

Bent u geïnteresseerd of wilt u meer informatie, neem dan contact op met ons via info@pinewood.nl of op tel.nr. (015) 251 36 36.